Chapter 10
Factors Influencing Information Security Policy Compliance Behavior

Kwame Simpe Ofori

https://orcid.org/0000-0001-7725-9756

School of Management and Economics, University of Electronic Science and Technology of China, China

Hod Anyigba

Nobel International Business School, Ghana

George Oppong Appiagyei Ampong

Department of Management, Ghana Technology University College, Ghana

Osaretin Kayode Omoregie

Department of Finance, Lagos Business School, Pan-Atlantic University, Nigeria

Makafui Nyamadi

Department of Operations and Information Systems, Business School, University of Ghana, Ghana

Eli Fianu

Ghana Technology University College, Ghana

ABSTRACT

One of the major concerns of organizations in today's networked world is to unravel how employees comply with information security policies (ISPs) since the internal employee has been identified as the weakest link in security policy breaches. A number of studies have examined ISP compliance from the perspective of deterrence; however, there have been mixed results. The study seeks to examine information security compliance from the perspective of the general deterrence theory (GDT) and information security climate (ISC). Data was collected from 329 employees drawn from the five top-performing banks in Ghana and analyzed with PLS-SEM. Results from the study show that security education training and awareness, top-management's commitment for information security, and peer non-compliance behavior affect the information security climate in an organization. Information security climate, punishment severity, and certainty of deterrent were also found to influence employees' intention to comply with ISP. The implications, limitations, and directions for future research are discussed.

INTRODUCTION

"Data breaches keep happening. So why don't you do something? – The New York Times"

Worldwide IT security spending was poised to increase to $124 billion dollars in 2019 from $71.1 billion in 2017 (Gartner, 2018; Hwang et al., 2017). Big ticket cases of data breaches in 2017 and 2018 more than ever, highlighted the need for better systems and controls to curtail and contain data protection contraventions. Both small and large companies like Yahoo, AT&T Citi Bank, JP Morgan, and Equifax have all fallen prey to data protection problems, internally (New York Times, 2018). Data compliance has become a key competitive resource employed by firms to outpace their competitors – typically involving the adoption and use of security policy initiatives (Kim & Kim, 2017). It is therefore by no means an understatement when reiterated that information security and its application is pivotal to the firms growth and success (Doherty et al. 2009). Furthermore, clarity has been established that the human element is major cause of information security breachesin organizations. In other words information security policy behavior is key to improving information security levels in organizations (Balozian & Leidner, 2017).

Prior research has attempted to explain information security policy breaches through the General Deterrence Theory (Chan et al., 2005; Donalds & Osei-Bryson, 2020; C. Lee et al., 2016; S. M. Lee et al., 2004), Theory of Planned Behavior, Protection Motivation Theory and Organizational Theory (Rajab & Eydgahi, 2019). While organizational theory focuses on the effect of security climate on security policy compliance (Chan et al., 2005), deterrence theory highlights the effect of user awareness of IS security countermeasures on perceived certainty and severity of organizational sanctions (D'Arcy et al., 2009). According to the literature, one key way to encourage and motivate employees to comply with Information Security Policy (ISP) is the enforcement of sanctions under the general deterrence theory framework (GDT) (Aurigemma & Mattson, 2017). The GDT framework embraces disinsentives that match appropriate sanctions to violators of the ISP (Wall et al., 2013). In other words, if employees perceive that there are harsh penalties once they are caught violating information systems security policy; they are less likely to violate information systems security policy (Cheng et al., 2013). Further, Diver (2007) opines that understanding and interpreting the effects of sanctions are critical because employee non-compliance is typically the mainspring of all ISPs. This therefore almost certainly addresses the relevance of the GDT in enforcing ISP. As maintained by the literature, another major compliance attribute – information security climate – has been found to have significant impact on compliance because workplace quality devoid of anti-compliance behavior is driven by the nature of peer socialization in the organization (Yazdanmehr & Wang, 2016). Although studies on GDT and security climate have laid solid foundation in the field, they have largely been inconclusive with respect to compliance (Chen et al., 2018; D'Arcy et al., 2009; Herath et al., 2018; Herath & Rao, 2009; Safa et al., 2019).

Clearly, there is a lack of coherence on the integration of general deterrence theory (GDT) – a theory that speaks to compliance bahavior and organizational Information Security Climate (ISC). In this study, we use the GDT as a foundation to build an integrated information security policy compliance behavior model that incorporates critical turnaround factors: Information Security Climate (ISC), Intention to Comply (INT) and GDT constructs. This research attempts to provide a systematic insight of the factors affecting information security policy compliance. In particular, an attempt to highlight key antecedent factors affecting policy compliance behavior in order to enhance organizational capabilities of safeguarding systems to enhance productivity and security. Specifically, these factors can contribute to enhanced

Related Content

Dimensions of Privacy Concerns Amongst Online Buyers in India
Tinu Jainand Prashant Mishra (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications (pp. 1214-1229).*
www.irma-international.org/chapter/dimensions-of-privacy-concerns-amongst-online-buyers-in-india/228779

Taxonomy of Login Attacks in Web Applications and Their Security Techniques Using Behavioral Biometrics
Rizwan Ur Rahmanand Deepak Singh Tomar (2020). *Modern Theories and Practices for Cyber Ethics and Security Compliance (pp. 122-139).*
www.irma-international.org/chapter/taxonomy-of-login-attacks-in-web-applications-and-their-security-techniques-using-behavioral-biometrics/253666

Demystifying Ransomware: Classification, Mechanism and Anatomy
Aaeen Naushadahmad Alchiand Kiranbhai R. Dodiya (2023). *Perspectives on Ethical Hacking and Penetration Testing (pp. 171-192).*
www.irma-international.org/chapter/demystifying-ransomware-classification-mechanism-and-anatomy/330264

For Better or for Worse?: Ethical Implications of Generative AI
Catherine Hayes (2024). *Exploring the Ethical Implications of Generative AI (pp. 104-120).*
www.irma-international.org/chapter/for-better-or-for-worse/343701

Security and Ethical Concerns of Affective Algorithmic Music Composition in Smart Spaces
Abigail Wiafeand Pasi Fränti (2020). *Modern Theories and Practices for Cyber Ethics and Security Compliance (pp. 193-203).*
www.irma-international.org/chapter/security-and-ethical-concerns-of-affective-algorithmic-music-composition-in-smart-spaces/253670